

REMARKS/ARGUMENTS

Claims 1-20 are pending. Claims 1 – 20 stand rejected. By the present amendment, Claim 1 has been amended. Reconsideration of the subject application is respectfully requested.

***Rejection of Claim 1 under 35 USC 103(a)
as being unpatentable over Wasilewski (U.S. Patent 6,424,714)***

Claim 1 stands rejected under 35 USC 103(a) as being unpatentable over Wasilewski. Claim 1 has been amended to clarify the differences between Wasilewski and the present invention. Claim 1 having been amended, this rejection is traversed because: (1) Wasilewski fails to teach each of the limitations recited in amended Claim 1; and (2) no motivation exists for modifying the teachings of Wasilewski to meet the limitations of Claim 1, absent impermissible use of hindsight gleaned from Applicant's own disclosure.

35 U.S.C. §103(a) sets forth in part:

[a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art (See MPEP §2143.03). Further, there must be some suggestion or motivation, and reasonable expectation of success, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings (See MPEP §706.02(j)).

Amended Claim 1 recites

A method for managing access to a scrambled event of a service provider, said method comprising:

(a) receiving in a device an electronic list of events, at least one event having an encrypted message associated therewith, said encrypted message comprising *a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to said associated event*;

(b) receiving in said device, in response to user selection of said event, said encrypted message;

(c) *decrypting said encrypted message to obtain said descrambling key*;

(d) receiving said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event; and

(e) *descrambling said selected event using said descrambling key. (Emphasis added).*

The Wasilewski reference fails to teach or suggest each of the limitations recited in present Claim

1. As an initial matter, the present Office action admits “Wasilewski does not expressly disclose indicating the events that are available to the customer in the form of an electronic list of events.” (see 7/30/2004 Office action, par. 1). However, in an attempt to remedy this admitted shortcoming of Wasilewski, the present Office action argues it would have been obvious “to indicate [to] the customer the types of events that are available in the form of a list of events.” (see 7/30/2004 Office action, par. 1). Applicant traverses this assertion. However, even assuming arguendo the above position of the Examiner, the system of Wasilewski nevertheless fails to teach or suggest the additional limitations of “receiving in a device an electronic list of events, at least one event having an encrypted message associated therewith, said encrypted message comprising a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to said associated event” as recited in amended Claim 1. Support for this limitation may be found, for example, in lines 10 – 15, on page 11 of Applicant’s specification, which recites:

After STB 100 authenticates EPG 580, the encrypted message is

passed to SC 420 for decryption. SC 420 decrypts the message using KSCpri, which is stored therein, to obtain the data corresponding to the selected event and the event key. This data may include data relating to channel identity, date and time stamp, event identity, and payment amount.

The claimed method further requires that the encrypted message containing both the descrambling key and event information is decrypted to retrieve the descrambling key (step c), which key is then used to descramble the selected event (step e). The Wasilewski reference does not teach or suggest an encrypted message, which message includes a descrambling key and the recited event information.

The system of Wasilewski teaches a control system that provides secure transmission of programs between a service provider and a customer's set top unit. Wasilewski uses three functional levels of encryption protection to accomplish its secure program transmission. At a first level, program-bearing MPEG-2 transport packets are encrypted using random number generated keys known as control words, to provide an encrypted program as illustrated in col. 8, lines 9 – 12 and block 154 of Fig. 3 of the drawings. At a second level, the control words are encrypted using a second randomly generated key called a multi-session key (MSK), as indicated in col. 8, lines 12 – 13 and block 153 of Fig. 3. At a third level, the MSK is encrypted using public key cryptography as provided for in col. 8, lines 13 – 16 and illustrated in blocks 30, 300 and 400 of Fig. 3. These three levels of encrypted data are then multiplexed into an MPEG-2 stream providing for conditional access as shown in block 52 of FIG. 3.

Nowhere does Wasilewski teach or suggest the recited encrypted message of Claim 1, which encrypted message comprises both a descrambling key and event information corresponding to said associated event. In contrast, a detailed review of the Wasilewski reference reveals that Wasilewski merely teaches encrypting a control word using a multi-session key (MSK) as discussed above for functional level two protection. Wasilewski clearly fails to teach or suggest the limitation of an encrypted message comprising both a descrambling key and event information corresponding to said associated

event.

Further study of Wasilewski reveals that neither the first nor third encryption levels provide for an encrypted message that is decrypted to obtain a key that is used to descramble received content – which is expressly required by Claim 1. Although Wasilewski discloses a message authentication code (MAC) and system-wide pay per view access information and copy protection information is appended to the encrypted control word in the second level of protection prior to transmission to a set top unit, Wasilewski expressly teaches this information is to be sent in the clear (i.e., not encrypted using the MSK). Accordingly, such data is not and cannot be part of the “encrypted message”. Further, Wasilewski clearly teaches the MAC and system-wide pay per view access information, copy protection information and the like are merely used in a hashing algorithm to authenticate the encrypted code word prior to releasing the same for decrypting (See, e.g. col. 9, lines 39 – 57).

Accordingly, a detailed reading of Wasilewski reveals that the reference fails to disclose or suggest significant aspects of independent method Claim 1 – in at least that it fails to teach, or suggest a method for managing access to a scrambled event of a service provider, said method of comprising: (a) receiving in a device an electronic list of events, at least one event having an encrypted message associated therewith, *said encrypted message comprising a descrambling key and at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to said associated event*;...*(c) decrypting said encrypted message to obtain said descrambling key*...and (e) *descrambling said selected event using said descrambling key. (Emphasis added).*

For the foregoing reasons, amended Claim 1 is not rendered obvious in view of Wasilewski, even assuming *arguendo* that it would have been obvious to utilize a list of events to indicate the types of events that are available to a customer in combination with the system of Wasilewski. Withdrawal of this 35 USC 103(a) rejection is respectfully requested.

The above notwithstanding, no motivation exists for somehow modifying the teachings of Wasilewski in an attempt to arrive at the invention as recited in present Claim 1. First, Wasilewski shows that the code words, the MSK, and protected content itself are all transmitted together (see Fig. 3 of the drawings). Thus, only a single, iterative connection exists between a service provider and a set top unit according to Wasilewski. (See, col. 9, lines 1 – 4). The protected content is delivered with the control words and MSK of Wasilewski, such that all of the information necessary to decrypt and display the protected content is present with the content. Wasilewski does not even hint at adding event information or additional overhead data in the form of channel identity, date and time stamp, event identity and/or payment amount.

Second, Wasilewski teaches the desirability of providing enhanced encryption through the use of the third level of protection, for information that does not change rapidly (See, e.g., col. 10, lines 10 – 14). In Applicant's invention, the event information including a channel identity, date and time stamp, event identity and payment amount corresponding to an associated event, does not change rapidly in the manner of the code words according to Wasilewski. Hence, to the extent one would be motivated to include this type of information in the system of Wasilewski, (a position Applicant traverses), such motivation would require inclusion in the third level of protection and not the second level, which encrypts the code words. Moreover, decrypting the third level of protection does not obtain a key that is used to descramble the protected content. Accordingly, nothing in Wasilewski suggests the desirability to include the features and limitations recited in present Claim 1, absent impermissible hindsight gleaned from Applicant's invention. The Pinder and Vancelette references similarly fail to cure the above-identified deficiencies of the primary reference.

Accordingly, as Wasilewski fails to teach or suggest each of the features and limitations of

present Claim 1, and further, as no motivation exists for modifying the teachings of Wasilewski to include such features and limitations, absent using impermissible hindsight, a prima facie case of obviousness is not established. Reconsideration and withdrawal of the 35 USC 103(a) rejection of Claim 1 is thus respectfully requested. Furthermore, claims 2-14 are dependent upon and include all the limitations of Claim 1, as well as other novel limitations, and should therefore also be considered allowable.

***Rejection of Claims 15, 18 under 35 USC 103(a) as being unpatentable
over Wasilewski in view of Pinder et al (U.S. Patent 5,742,677)***

Claims 15 and 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Pinder. Applicant respectfully requests reconsideration and removal of the rejections of these Claims for at least the following reasons.

Independent Claim 15 recites:

A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

- (a) receiving an electronic program guide from a guide provider, said guide having a message and a digital signature associated with each event in said guide, *said message being encrypted using a public key of the smart card and said digital signature being created using a private key of said guide provider;*
- (b) selecting an event from said guide;
- (c) receiving said encrypted message and said digital signature corresponding to the selected event;
- (d) authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device;
- (e) passing said message to said smart card;
- (f) *decrypting, in said smart card, said message using a private key of said smart card to obtain event information and a symmetric key, said smart card private key being stored within said smart card;*
- (g) storing said event information in said smart card and updating account information based on said event information;
- (h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i) *descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event. (Emphasis added).*

In similar fashion to Claim 1 discussed above, Claim 15 recites, in part, decrypting an encrypted message to obtain event information and a symmetric key, which symmetric key is then used to descramble an event. While the Wasilewski reference may teach encrypting control words using a multi-session key (MSK), it does not teach an encrypted message that comprises a descrambling key and event information. Thus, the arguments discussed hereinabove with regard to claim 1 also apply to present independent Claim 15. Moreover, the Pinder reference does nothing to overcome the deficiencies associated with Wasilewski discussed above.

In addition, present Claim 15 further recites a symmetric key encrypted using public key cryptography. In contradistinction, Wasilewski expressly teaches against using public key cryptography to encrypt the code words and instead relies upon a second randomly generated key, i.e., the MSK (see col. 8, lines 6 – 13 of Wasilewski). In fact, Wasilewski teaches only using public key cryptography in the third level of protection, i.e., for information that does not change as rapidly as do the code words (see col. 10, lines 10 – 14).

Accordingly, as the claimed invention recites features and limitations contrary to the teachings of the primary reference, any purported modification of Wasilewski is entirely without motivation or suggestion in the reference itself and hence, represents impermissible hindsight. For at least these additional reasons, reconsideration and withdrawal of this 35 USC 103(a) rejection is respectfully requested. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 16 and 17 as well, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 15.

With regard to independent Claim 18, it recites:

A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

- (a) receiving an electronic program guide from a guide provider, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said digital certificates being encrypted using a first private key of said guide, *said separate message being encrypted using a public key of the smart card* and having an associated digital signature created using a second private key of said guide;
- (b) selecting an event from said guide;
- (c) receiving said digital certificate, said message and said digital signature corresponding to the selected event;
- (d) authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and decrypting said digital signature using said second guide public key, said first guide public key being stored in the device;
- (e) passing said message to said smart card;
- (f) *decrypting, in said smart card, said message using a private key of the smart card to obtain event information and a symmetric key*, said smart card private key being stored within the smart card;
- (g) storing said event information in the smart card and updating account information based on said event information;
- (h) receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and
- (i) *descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event. (Emphasis added).*


As discussed above, none of the cited references of record, either alone or in combination, teach or suggest each of the recited features and limitations of present Claim 18. Reconsideration and removal of the rejection of Claim 18 is requested for at least the reasons set forth with regard to Claims 1 and 15. Applicant also requests reconsideration and removal of the rejections of Claims 19 and 20 as well, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 18.

U.S. Serial No. 09/445,133
Attorney Docket No. RCA-88674

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, Claims 1-20 of this application stand in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully Submitted

Date: Jan 21, 2005



Paul Kiel
Registration No. 40,677

THOMSON LICENSING INC.
Patent Operations
CN 5312
Princeton, NJ 08543-0028